DATA PROTECTION AND PACKET MODE IN THE DISTRIBUTED INFORMATION MEASUREMENT AND CONTROL SYSTEM FOR RESEARCH IN PHYSICS

Sergey Kiprushkin, Nikolay Korolev, Sergey Kurskov, Vadim Semin

Abstract: The present paper is devoted to creation of cryptographic data security and realization of the packet mode in the distributed information measurement and control system that implements methods of optical spectroscopy for plasma physics research and atomic collisions. This system gives a remote access to information and instrument resources within the Intranet/Internet networks. The system provides remote access to information and hardware resources for the natural sciences within the Intranet/Internet networks. The access to physical equipment is realized through the standard interface servers (PXI, CAMAC, and GPIB), the server providing access to Ethernet devices, and the communication server, which integrates the equipment servers into a uniform information system. The system is used to make research task in optical spectroscopy, as well as to support the process of education at the Department of Physics and Engineering of Petrozavodsk State University.

Keywords: distributed information measurement and control system, equipment server, PXI server, CAMAC server, GPIB server, distance learning.

ACM Classification Keywords: H.3.4 Systems and Software: Distributed systems.

Conference: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008

Introduction

A distributed information measurement and control system was implemented at the Department of Physics and Engineering of Petrozavodsk State University (Russia) to fortify research in the field of optical spectroscopy and facilitate academic activities [Gavrilov et al, 2003], [Kiprushkin et al, 2004 – 2005].

The system is quit unique because it integrates various tool interfaces into one network functioning on the basis of the TCP/IP protocol stack.

The client-server technology was chosen as the key element of the system; in addition, an application protocol [Гаврилов et al, 2002] over the TCP/IP was developed to access physical experimental equipment – which enables the system to function in the Intranet/Internet networks. It was necessary to create our own protocol because common Web-technologies lack flexibility in experiment monitoring since, in this case, experimental procedures are run by executable codes, saved on the computer directly connected to the experimental setup, rather than client programs [e.g. Зимин et al, 2006]

The heterogeneous system includes client programs, that run the experiment, a communication server, the key element of the system, equipment servers (CAMAC server [Zhiganov et al, 2000], GPIB server [Кашуба et al, 2002], PXI Server, Intel MCS-196 microcontroller server, the Ethernet devices server [Kiprushkin, Kurskov, Sukharev, 2007], the server of access to GDS-840C digital oscilloscope etc.), measuring and execution units of the experimental setup, and a database server [Kiprushkin, Kurskov, Semin, 2007]. The scheme of the distributed information measurement and control system is presented in Figure 1.

Output protocoling and database storing are realized on the basis of DBMS Oracle 9i. Client programs call it directly, bypassing the client server, because the latter has no information on the type of the ongoing experiment.

The communication server, the equipment servers, and client programs are realized as Java applications. The data exchange among them is based on TCP stream sockets provided by Java.net information packet, which is

included into Java API standard packet. The methods of using the input-output ports for the access to the interface controllers are written in C programming language.

Administration of the distributed system is based on server-side Java servlet.

The goal of this project was to switch the information measurement and control system to the SSL protocol (Secure Socket Layer) and to upgrade it with the packet mode.

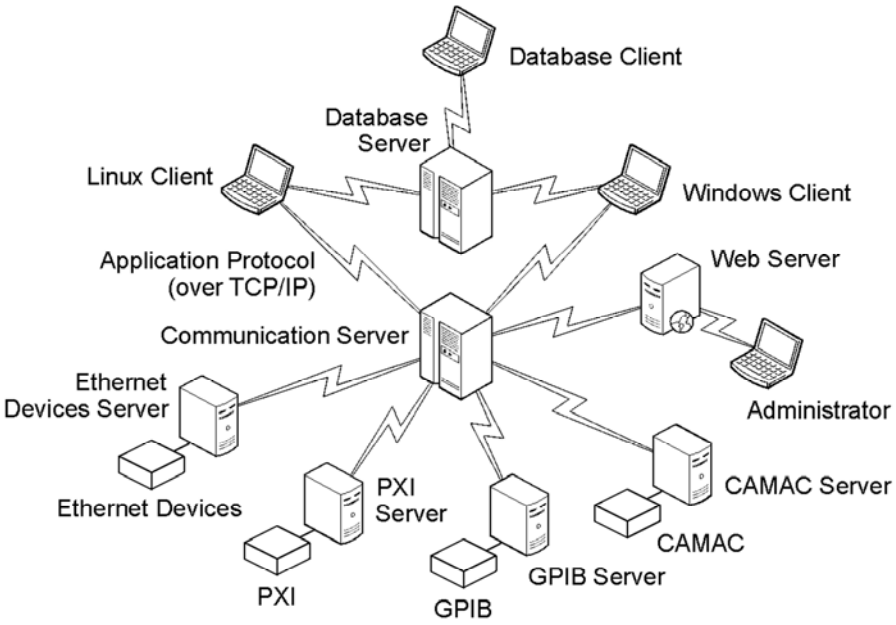

Figure 1. The scheme of the distributed information measurement and control system

Data Protection

The SSL protocol is a standard protocol based on the TCP/IP protocol stack with an encrypted connection between the client and the server. The SSL protocol follows invariable communication security steps – which are an advantage and a disadvantage – on the one hand, it operates time-proven methods, on the other hand, there is often a lack of flexibility when it comes to develop a unique system that requires more advanced methods. It is crucial to note that the majority of modern software products support the SSL protocol – that reflects a growing importance of security in information technologies.

The SSL protocol is a connection protocol developed by Netscape Communications Corporation. It runs over the TCP/IP. The SSL protocol provides confidentiality via data encryption, protection of data integrity with Message Authentication Code (MAC), client and server authentication and validity. The SSL protocol may be used by higher-level protocols such as, for example, the HTTP. The SSL protocol Version 1 did not become popular while Version 2 was introduced by the Netscape Company in the first version of Netscape Navigator. The third version of this protocol is the most modern and widely-spread. The TLS protocol (Transport Layer Security) developed by the Internet Engineering Task Force (IETF), broadens capabilities of the SSL protocol Version 3 regarding authentication. The WTLS protocol (Wireless Transport Layer Security) is a version of the TLS protocol for wireless networks.

The developed system of cryptographic security of the information measurement and control system is double-leveled in terms of security policies. The communication server works as a core element that distributes secret keys and authenticates all public keys. It is an issuer, i.e. it issues certificates to public keys. It is completely trusted. A certificate is a means of client and server authentication when establishing the connection. A certificate is a block of data that contains information required for principal's identification. This information contains

principal's public key, information on the principal, period of validity of the certificate, issuer's information signature.

Java 2 has a keytool utility that allows monitoring of keystores. The keystores contain generated keys and trusted certificates. Key generation is a private key plus a sequence of X.509 certificates that authenticates a corresponding public key. The keytool utility does not support symmetric keys; instead, during an SSL connection a secret session key (temporary keys) is generated for traffic encryption.

Data security in the system is based on Java Secure Socket Extension (JSSE), that is, basically, a standard API-interface for the SSL protocol versions 2 and 3 and the TLS protocol (class library – file jsse.jar). Cryptographic features of the SSL protocol are hidden from the programmer.

Client and server applications that use the SSL protocol based on SSL-sockets are generated in a similar way: the route to the keystore location, its type and password as well as a certificate authority and trusted certificate authorities are indicated in the program. The utility keytool facilitates generation and use of key stores. It enables a user to set the following parameters of a key: an alias, an encryption algorithm, a size, validity, and a keystore location. Option defaults are as follows: -alias "mykey", -keyalg "DSA", -keysize 1024, -validity 90, -keystore the file named keystore in the user's home directory. If the main algorithm is of type "DSA", the signature algorithm option defaults to "SHA1withDSA". If the underlying main algorithm is of type "RSA", -the signature algorithm defaults to "MD5withRSA".

To establish an SSL-connection, the server and the client first have to export public keys' certificates to the file, then exchange and import them to their keystores.

The use of SSL-sockets reduces the costs of encrypted communications and broadens capabilities of the system. Whereas, one of the disadvantages is that SSL-sockets do not support all cryptographic algorithms.

The former cryptographic classes [Kiprushkin, Korolev, Kurskov, 2005] developed for this system are still of importance because they can be used to secure cryptographically almost any information measurement system.

Packet Mode of Distributed System

As for the second part of this project, it is necessary to point out that client-server architecture enables users (clients) to get a secure access to information, independent from hardware and software combinations. The client-server model fortifies the use of new automation technologies, brings data processing closer to the client, simplifies the use of graphic interfaces and transition to open systems.

However, an experimental complex can be run directly by the commands of a client program only if the connection is secure and the network capacity is sufficient. Otherwise, there is a risk that the experiment will be delayed or results lost.

The packet mode enables the program to send the client command packets instead of single commands.

The packet mode makes it possible to reduce data volume transmitted over the net as well as shorten the timing of useful data transmission. This is crucial when organizing distance lab activities for students studying off campus.

To realize the packet mode, we developed modules (classes) that allow transmission and processing of blocks of commands. In addition, method libraries of equipment servers connected to physical setups were upgraded with methods that do not require client's interference in experimental measurements (for example, a procedure of setting up the monochromator to the chosen wave length or measuring the impulse counting rate from the photomultiplier tube).

Let us take a closer look at how the system functions in a standard mode and a packet mode (without considering security procedures).

In a standard mode, a client asks a server to reserve a resource. Then, a communication server verifies that an equipment server has this resource and that is not being used by another client. Depending on the output, the server responds to the client that the resource is available, being used by another user reserved by this user or

does not exist. If the resource is available, the client sends the first command to the communication server, the latter checks and forwards it to the equipment server. The equipment server, having processed the command, sends the output to the communication server that sends it then back to the client. After that, the client may send the next command. Having done working with the resource, the client sends the communication server a command that the resource is available.

The system works differently in a packet mode. In the beginning, just like in a standard mode, a resource is reserved. After that, the client communicates to the server that packet transmission is initiated. Following this command, the communication server starts to send the equipment server the commands received from the client without waiting for them to be executed. The equipment server, having received a packet transmission begin command, stores all consecutive commands in a file until the packet transmission is over. After that, the equipment server starts to execute the commands reading them from the file. At this time, the client may disconnect from the communication server since there is no need to remain connected. When the server has finished executing the commands, the client can ask it to send an output packet.

Command or output packet transfer is run by single frames with a server or a client confirming the reception of each frame.

During the development of the packet mode, the interface of the communication server CServerProtocol was upgraded with the following commands:

- CS_GETHSERVERSTATUS – check the status of the addressed equipment server;
- CS_RECEIVEPACKET – a command that switches the communication server to the receive packet mode (begin packet) ;
- CS_ENDPACKET – a command that ends packet transmission (end packet);
- CS_SENDPACKET – send an output packet.

Likewise, the commands of equipment servers were upgraded with the commands that do not require any response from a running client program. For the CAMAC server they are as follows:

- CMS_WRITE_WITH_L – write data and wait for L-request;
- CMS_WAIT_L – wait for L-request;
- CMS_CHECK_Q – check the status of signal Q;
- CMS_BEGIN_LINE – set up the monochromator to the chosen wave length;
- CMS_SPECTRUM – register the spectrum in a set wave length diapason;
- CMS_FUNCTION – write the excitation function of a spectral line in a set diapason of energy collisions;
- et al.

Commands stop running and communicate an error if there is no L-request within a set time period.

Conclusion

This distributed information measurement and control system is based on the modular approach implemented both in the structure and in the software. Clients and equipment servers are built into the system according to the unified rules and interact on a unified protocol by the principles of open systems. Note that an open system is a system that implements open specifications or standards for interfaces, services and formats in order to provide software portability with minimal changes in a wide range of systems (mobility) as well as interaction with other applications on local or remote systems (interoperability) and users (user mobility). In particular, distributed systems are based on OSE/RM model that describes systems by client/server architecture.

The use of the SSL protocol working over the TCP/IP protocols in data encryption significantly simplified traffic encryption between a client and a server ensuring information integrity and confidentiality. The SSL protocol is

particularly worth-using in distributed information measurement and control systems that are normally utilized in research and academic labs with less strict data and equipment security requirements.

As for the developed packet mode, it considerably increases system security in general by preventing experimental data loss due to lost connection with the client and reduces network load.

It is necessary to point out that the developed distributed information measurement and control system is used for the beam and plasma object analysis with the help of optical spectroscopy methods [Kurskov et al, 2006], [Кашуба, 2006]. In particular, the researches on excitation processes of atomic collisions with inert gas atoms' participation are carried out with its help as well as the laboratory works with senior students of the Department of Physics and Engineering of Petrozavodsk State University.

Acknowledgments

We would like to express our gratitude to the laboratories' Head I. P. Shibaev for support of this work as well as engineers A. N. Cykunov and A. V. Mandychev, and Masters of Philosophy M. A. Gvozd, V. G. Mullamekhametov, and D. V. Korolev.

The research described in this publication was made possible in part by Award of the U.S. Civilian Research & Development Foundation (CRDF) and of the Ministry of Education and Science of Russian Federation.

Conclusion

This exemplar is meant to be a model for manuscript format. Please make your manuscript look as much like this exemplar as possible.

In the case of serious deviations from the format, the paper will be returned for reformatting.

Bibliography

[Gavrilov et al, 2003] S.E.Gavrilov, S.A.Kiprushkin, S.Yu.Kurskov. Distributed information system with remote access to physical equipment. In: Proceedings of the International Conference on Computer, Communication and Control Technologies: CCCT '03 and The 9th International Conference on Information Systems Analysis and Synthesis: ISAS'03. Orlando, 2003.

[Kiprushkin et al, 2004] S.A.Kiprushkin, N.A.Korolev, S.Yu.Kurskov. Data security in the distributed information measurement system. In: Proceedings of the 8th World Multi-Conference on Systemics, Cybernetics and Informatics: SCI 2004. Orlando, 2004, Vol. 1, pp. 13-16.

[Kiprushkin et al, 2005] S.A.Kiprushkin, S.Yu.Kurskov, N.G.Nosovich. Resources Control in Distributed Information Measurement System. In: Proceedings of the 3rd International Conference on Computing, Communication and Control Technologies: CCCT '05. Austin, Texas, USA, 2005.

[Kiprushkin et al, 2005] S.A.Kiprushkin, N.A.Korolev, S.Yu.Kurskov. Sharing of Instrument Resources on the Basis of Distributed Information Measurement System. In: Proceedings of the Second IASTED International Multi-Conference on Automation, Control, and Information Technology – Automation, Control, and Applications: ACIT-ACA 2005. Novosibirsk, ACTA Press, 2005, pp. 170-175.

[Гаврилов et al, 2003] С.Е.Гаврилов, Е.Д.Жиганов, С.А.Кипрушкин, С.Ю.Курсков. Распределенная информационно-измерительная система для удаленного управления экспериментом в области оптической спектроскопии". Труды Всероссийской научной конференции Научный сервис в сети Интернет 2002. Москва, Издательство Московского государственного университета, 2002, сс. 157–159.

[Зимин et al, 2006] А.М.Зимин, Б.В.Букеткин, А.П.Почуев и др. Учебная Интернет-лаборатория "Испытания материалов". Информационные технологии, No. 10, 2006, сс. 58–65.

[Zhiganov et al, 2000] E.D.Zhiganov, C.A.Kiprushkin, S.Yu.Kurskov. CAMAC Server for Remote Access to Physical Equipment. In: Learning and Teaching Science and Mathematics in Secondary and Higher Education. Joensuu, University of Joensuu, 2000, pp. 170–173.

[Кашуба et al, 2002] А.С.Кашуба, С.А.Кипрушкин, С.Ю.Курсков. Сервер канала общего пользования распределенной информационной системы поддержки научных исследований в области оптической спектроскопии. В: Технологии

информационного общества – Интернет и современное общество 2002 (IST/IMS 2002): Материалы V Всерос. объединенной конф. Санкт-Петербург, Издательство С.-Петербургского университета, 2002, сс. 104–105.

[Kiprushkin, Kurskov, Sukharev, 2007] S.Kiprushkin, S.Kurskov, E.Sukharev. Connection of network sensors to distributed information measurement and control system for education and research. International Journal "Information Technologies & Knowledge", Vol. 1, No. 2, 2007, pp. 171–175.

[Kiprushkin, Kurskov, Semin, 2007] S.Kiprushkin, S.Kurskov, V.Semin. Development of database for distributed information measurement and control system. In: Proceedings of the International Conference "e-Management & Business Intelligence": eM&BI 2007, Bulgaria, Eds.: Kr.Markov, Kr.Ivanova. Sofia, Institute of Information Theories and Applications FOI ITHEA, 2007, pp. 48–51.

[Kurskov, 2006] S.Yu.Kurskov, A.D.Khakhaev. On mechanisms of He I collisional excitation in He-He system. Czechoslovak Journal of Physics, Vol. 56, 2006, pp. B297–B302.

[Кашуба, 2006] А.С.Кашуба. Проблемно-ориентированная распределенная информационно-измерительная и управляющая система для изучения процессов возбуждения при столкновениях тяжелых частиц. Системы управления и информационные технологии, No. 4.2 (26), 2006, сс. 234–238.

Authors' Information

Sergey Kiprushkin – Senior lecturer, Petrozavodsk State University, Department of Physics and Engineering, Lenin Ave., 33, Petrozavodsk-185910, Russia; e-mail: skipr@dfe3300.karelia.ru

Sergey Kurskov – Associate professor, Petrozavodsk State University, Department of Physics and Engineering, Lenin Ave., 33, Petrozavodsk-185910, Russia; e-mail: kurskov@psu.karelia.ru

Nikolay Korolev – Researcher, Petrozavodsk State University, Department of Physics and Engineering, Lenin Ave., 33, Petrozavodsk-185910, Russia; e-mail: kna@sampo.ru

Vadim Semin – PhD student, Petrozavodsk State University, Department of Physics and Engineering, Lenin Ave., 33, Petrozavodsk-185910, Russia; e-mail:semin@psu.karelia.ru